

On a restricted linear congruence

Khodakhast Bibak ^{*} Bruce M. Kapron ^{*} Venkatesh Srinivasan ^{*†}

October 26, 2016

Abstract

Let $b, n \in \mathbb{Z}$, $n \geq 1$, and $\mathcal{D}_1, \dots, \mathcal{D}_{\tau(n)}$ be all positive divisors of n . For $1 \leq l \leq \tau(n)$, define $\mathcal{C}_l := \{1 \leq x \leq n : (x, n) = \mathcal{D}_l\}$. In this paper, by combining ideas from the finite Fourier transform of arithmetic functions and Ramanujan sums, we give a short proof for the following result: the number of solutions of the linear congruence $x_1 + \dots + x_k \equiv b \pmod{n}$, with $\kappa_l = |\{x_1, \dots, x_k\} \cap \mathcal{C}_l|$, $1 \leq l \leq \tau(n)$, is

$$\frac{1}{n} \sum_{d|n} c_d(b) \prod_{l=1}^{\tau(n)} \left(c_{\frac{n}{\mathcal{D}_l}}(d) \right)^{\kappa_l},$$

where $c_d(b)$ is a Ramanujan sum. Some special cases and other forms of this problem have been already studied by several authors. The problem has recently found very interesting applications in number theory, combinatorics, computer science, and cryptography. The above explicit formula generalizes the main results of several papers, for example, the main result of the paper by Sander and Sander [J. Number Theory **133** (2013), 705–718], one of the main results of the paper by Sander [J. Number Theory **129** (2009), 2260–2266], and also gives an equivalent formula for the main result of the paper by Sun and Yang [Int. J. Number Theory **10** (2014), 1355–1363].

Keywords: Restricted linear congruence; Ramanujan sum; finite Fourier transform

2010 Mathematics Subject Classification: 11D79, 11P83, 11L03, 11A25, 42A16

1 Introduction

Recently, Bibak et al. [1] gave an explicit formula for the number of solutions of the linear congruence $a_1x_1 + \dots + a_kx_k \equiv b \pmod{n}$, with $(x_i, n) = t_i$ ($1 \leq i \leq k$), where $a_1, t_1, \dots, a_k, t_k, b, n$ ($n \geq 1$) are arbitrary integers. They called these kinds of congruences *restricted linear congruences*. Some special cases and other forms of this problem have been already studied by several authors. The problem has recently found very interesting applications in number theory, combinatorics, computer science, and cryptography. For example, the special case of $b = 0$, $a_i = 1$, $t_i = \frac{n}{m_i}$, $m_i | n$ ($1 \leq i \leq k$) is related to the *orbicyclic* (multivariate arithmetic) function [5], which has very interesting combinatorial and topological applications, in particular, in counting non-isomorphic maps on orientable surfaces [5]. Also, the problem has been applied in studying universal hashing [2] which has many applications in computer science. Specifically, using the explicit formula for the number of solutions of the above restricted linear congruence, we designed an almost-universal hash function family and gave some applications to authentication and secrecy codes [2].

Let $e(x) = \exp(2\pi ix)$ be the complex exponential with period 1. For integers m and n ($n \geq 1$) the quantity

$$c_n(m) = \sum_{\substack{j=1 \\ (j,n)=1}}^n e\left(\frac{jm}{n}\right) \quad (1.1)$$

^{*}Department of Computer Science, University of Victoria, Victoria, BC, Canada V8W 3P6. Email: {kbibak,bmkapron,srinivas}@uvic.ca

[†]Centre for Quantum Technologies, National University of Singapore, Singapore 117543.

is called a *Ramanujan sum*, which is also denoted by $c(m, n)$ in the literature. From (1.1), it is clear that $c_n(-m) = c_n(m)$. Also, it is easy to see that $c_n(m) = c_n((m, n))$, for every m, n .

In this paper, we prove the following theorem:

Theorem 1.1. *Let $b, n \in \mathbb{Z}$, $n \geq 1$, and $\mathcal{D}_1, \dots, \mathcal{D}_{\tau(n)}$ be all positive divisors of n . For $1 \leq l \leq \tau(n)$, define $\mathcal{C}_l := \{1 \leq x \leq n : (x, n) = \mathcal{D}_l\}$. The number of solutions of the linear congruence $x_1 + \dots + x_k \equiv b \pmod{n}$, with $\kappa_l = |\{x_1, \dots, x_k\} \cap \mathcal{C}_l|$, $1 \leq l \leq \tau(n)$, is*

$$\frac{1}{n} \sum_{d|n} c_d(b) \prod_{l=1}^{\tau(n)} \left(c_{\frac{n}{\mathcal{D}_l}}(d) \right)^{\kappa_l}. \quad (1.2)$$

The above theorem generalizes the main results of [3, 4, 7, 9], one of the main results of [8], and also gives an equivalent formula for the main result of [10]. Note that, recently, Bibak et al. [1] gave a different proof for an ‘equivalent’ form of Theorem 1.1. But here we combine ideas from the finite Fourier transform of arithmetic functions and Ramanujan sums to present a new and short proof for the above theorem with the hope that its idea might be applicable to other relevant problems. In fact, as problems of this kind have many applications, especially in computer science and cryptography, having generalizations and/or new proofs and/or equivalent formulas for this problem may lead to further work. We also remark that, recently, Yang and Tang [11] considered the quadratic version of this problem in the special case of $k = 2$, $a_1 = a_2 = 1$, $t_1 = t_2 = 1$, and posed some problems for more general cases.

2 Proof of the theorem

Before we proceed, we need some preliminaries. Let r be a positive integer. An arithmetic function f is called *periodic* with period r (or *periodic modulo r*) if $f(m+r) = f(m)$, for every $m \in \mathbb{N}$. From (1.1), it is clear that $c_n(m)$ is a periodic function of m with period n .

Let $f(m)$ be an arithmetic function with period n . The *finite Fourier transform* of f is defined to be the function

$$\widehat{f}(b) = \frac{1}{n} \sum_{m=1}^n f(m) e\left(\frac{-bm}{n}\right). \quad (2.1)$$

Then a Fourier representation of f is obtained as (see, e.g., [6, p. 109])

$$f(m) = \sum_{b=1}^n \widehat{f}(b) e\left(\frac{bm}{n}\right). \quad (2.2)$$

Now we are ready to give a short proof for Theorem 1.1.

Proof of Theorem 1.1. Suppose that $\widehat{f}_n(k, b)$ denotes the number of solutions of the linear congruence $x_1 + \dots + x_k \equiv b \pmod{n}$, with $\kappa_l = |\{x_1, \dots, x_k\} \cap \mathcal{C}_l|$, $1 \leq l \leq \tau(n)$. One can observe that, for every $m \in \mathbb{N}$, we have

$$\sum_{b=1}^n \widehat{f}_n(k, b) e\left(\frac{bm}{n}\right) = \prod_{l=1}^{\tau(n)} \left(\sum_{x \in \mathcal{C}_l} e\left(\frac{mx}{n}\right) \right)^{\kappa_l}. \quad (2.3)$$

First, we give a short combinatorial argument to justify (2.3). Here the key idea is that $\widehat{f}_n(k, b)$ can be interpreted as the number of possible ways of writing b as a sum modulo n of κ_1 elements of \mathcal{C}_1 , κ_2 elements of \mathcal{C}_2 , \dots , $\kappa_{\tau(n)}$ elements of $\mathcal{C}_{\tau(n)}$. Now, expand the right-hand side of (2.3). Note that each term of this expansion has $e(\frac{bm}{n})$ as a factor (compare this to the left-hand side of (2.3)). Also note that the exponent of each term of this expansion (ignoring m) is just a sum of some elements of $\mathcal{C}_1, \dots, \mathcal{C}_{\tau(n)}$, which equals b

($1 \leq b \leq n$). In fact, recalling the above interpretation of $\widehat{f}_n(k, b)$, we can see that in this expansion there are exactly $\widehat{f}_n(k, 1)$ terms of the form $e(\frac{m}{n})$, $\widehat{f}_n(k, 2)$ terms of the form $e(\frac{2m}{n})$, \dots , $\widehat{f}_n(k, n)$ terms of the form $e(m)$; that is, there are exactly $\widehat{f}_n(k, b)$ terms of the form $e(\frac{bm}{n})$, for $1 \leq b \leq n$. Therefore, we get the left-hand side of (2.3).

Putting $x'_l = \frac{x}{\mathcal{D}_l}$, $1 \leq l \leq \tau(n)$, we get

$$\sum_{x \in \mathcal{C}_l} e\left(\frac{mx}{n}\right) = \sum_{\substack{x=1 \\ (x, n) = \mathcal{D}_l}}^n e\left(\frac{mx}{n}\right) = \sum_{\substack{x'_l=1 \\ (x'_l, n/\mathcal{D}_l)=1}}^{n/\mathcal{D}_l} e\left(\frac{mx'_l}{n/\mathcal{D}_l}\right) = c_{\frac{n}{\mathcal{D}_l}}(m).$$

Therefore,

$$\sum_{b=1}^n \widehat{f}_n(k, b) e\left(\frac{bm}{n}\right) = \prod_{l=1}^{\tau(n)} \left(c_{\frac{n}{\mathcal{D}_l}}(m)\right)^{\kappa_l}.$$

Now, by (2.1) and (2.2), and since $c_{\frac{n}{\mathcal{D}_l}}(m) = c_{\frac{n}{\mathcal{D}_l}}((m, n))$, we have

$$\begin{aligned} \widehat{f}_n(k, b) &= \frac{1}{n} \sum_{m=1}^n e\left(\frac{-bm}{n}\right) \prod_{l=1}^{\tau(n)} \left(c_{\frac{n}{\mathcal{D}_l}}(m)\right)^{\kappa_l} \\ &= \frac{1}{n} \sum_{d|n} \sum_{\substack{m=1 \\ (m, n)=d}}^n e\left(\frac{-bm}{n}\right) \prod_{l=1}^{\tau(n)} \left(c_{\frac{n}{\mathcal{D}_l}}(m)\right)^{\kappa_l} \\ &= \frac{1}{n} \sum_{d|n} \sum_{\substack{m=1 \\ (m, n)=d}}^n e\left(\frac{-bm}{n}\right) \prod_{l=1}^{\tau(n)} \left(c_{\frac{n}{\mathcal{D}_l}}(d)\right)^{\kappa_l} \\ &\stackrel{m' = m/d}{=} \frac{1}{n} \sum_{d|n} \sum_{\substack{m'=1 \\ (m', n/d)=1}}^{n/d} e\left(\frac{-bm'}{n/d}\right) \prod_{l=1}^{\tau(n)} \left(c_{\frac{n}{\mathcal{D}_l}}(d)\right)^{\kappa_l} \\ &= \frac{1}{n} \sum_{d|n} c_{n/d}(-b) \prod_{l=1}^{\tau(n)} \left(c_{\frac{n}{\mathcal{D}_l}}(d)\right)^{\kappa_l} \\ &= \frac{1}{n} \sum_{d|n} c_{n/d}(b) \prod_{l=1}^{\tau(n)} \left(c_{\frac{n}{\mathcal{D}_l}}(d)\right)^{\kappa_l} = \frac{1}{n} \sum_{d|n} c_d(b) \prod_{l=1}^{\tau(n)} \left(c_{\frac{n}{\mathcal{D}_l}}(d)\right)^{\kappa_l}. \end{aligned}$$

□

Acknowledgements

The authors would like to thank the anonymous referees for helpful comments. During the preparation of this work the first author was supported by a Fellowship from the University of Victoria (UVic Fellowship).

References

- [1] K. Bibak, B. M. Kapron, V. Srinivasan, R. Tauraso, and L. Tóth, Restricted linear congruences, arXiv: 1503.01806.

- [2] K. Bibak, B. M. Kapron, V. Srinivasan, and L. Tóth, On an almost-universal hash function family with applications to authentication and secrecy codes, arXiv: 1507.02331.
- [3] E. Cohen, A class of arithmetical functions, *Proc. Natl. Acad. Sci. USA* **41** (1955), 939–944.
- [4] J. D. Dixon, A finite analogue of the Goldbach problem, *Canad. Math. Bull.* **3** (1960), 121–126.
- [5] V. A. Liskovets, A multivariate arithmetic function of combinatorial and topological significance, *Integers* **10** (2010), 155–177.
- [6] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I: Classical Theory*, Cambridge University Press, (2006).
- [7] C. A. Nicol and H. S. Vandiver, A von Sterneck arithmetical function and restricted partitions with respect to a modulus, *Proc. Natl. Acad. Sci. USA* **40** (1954), 825–835.
- [8] J. W. Sander, On the addition of units and nonunits mod m , *J. Number Theory* **129** (2009), 2260–2266.
- [9] J. W. Sander and T. Sander, Adding generators in cyclic groups, *J. Number Theory* **133** (2013), 705–718.
- [10] C.-F. Sun and Q.-H. Yang, On the sumset of atoms in cyclic groups, *Int. J. Number Theory* **10** (2014), 1355–1363.
- [11] Q.-H. Yang and M. Tang, On the addition of squares of units and nonunits modulo n , *J. Number Theory* **155** (2015), 1–12.